



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/643,069	08/18/2003	Alain Chateau	TI-33657	4187

23494 7590 03/06/2007
TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER

WILLIAMS, KENT L

ART UNIT	PAPER NUMBER
----------	--------------

2139

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 10/643,069	Applicant(s) CHATEAU ET AL.	
	Examiner Kent L. Williams	Art Unit 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 August 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 November 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>18 August 2003</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: "may stored" should be "may be stored" on page 1, line 14. "By cipher" should be "by a cipher" on page 2, line 4. "Storing a writing" should only be "storing" on page 2, line 17. "The random memory generator" should be "the random number generator" on page 5, line 22. The Examiner believes that "(encrypt before storage)" adjacent to "seed," on page 8, line 1, is misplaced within the sentence as a 'seed' is not used to encrypt data before storage. The Examiner believes that "(blowing all the fuses)" adjacent to "erasing," on page 6, line 21, is misplaced as blowing all the fuses would not be an outcome of blowing the "programming fuse" to prevent future programming or erasure.

Appropriate correction is required.

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: "Random Number and/or Key Generator on An Integrated Circuit."

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 2139

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 4, 5, 8 and 9 are rejected under 35 U.S.C. 102(b) as being anticipated by Fischer (U.S. Patent No. 5,422,953).

Claims 1, 5 and 9 recite the limitations of a Random Number Generator (RNG) within an Integrated Circuit (IC) and having a "permanent memory," accessible only within said IC, to store a generated random number. Claim 5 further recites the limitations of said IC containing "processing circuitry," and a "random key generator" comprising aforementioned RNG. Please note that "random number" and "random key" are interchangeable, as a random key *is* a random number in general (and always true in symmetrical cryptographic schemes) as used by Fischer and the instant application. Coupling of said RNG to the "processing circuitry," recited per claim 5, is also inherent within claims 1 and 9 by the limitation of limiting access to the "random number"/"random key." Fischer teaches the use of limited accessibility to said memory and generated values (e.g., random key/number) only within the IC as, "The secret private key storage 6 may, for example, be a secure RAM or a *write-once memory* [e.g., Programmable Read Only Memory (PROM)]. (Emphasis added, Column 3, lines 34-38)." Further, "Preferably the device 2 generates its own private key so that it never exists outside the confines of the secure notary device environment. (Column 4, lines 31-34)." Fischer, congruent with the instant application, teaches that a random number and a random key are synonymous as, "Any other random value generator may be used...to maximize the randomness of the value used by the *processor 4* in the *digital signature process*. (Emphasis added, Column 4, lines 5-7)." Digital signature

Art Unit: 2139

processes' use keys, where the key is the "value" or number generated by the RNG.

The processor mentioned is coupled to the Random Number Generator (or Random Value/Key Generator) per Figure 1, Blocks 4, 10, 6 and 8. Also, "[Fischer's] invention is embodied in a token device, e.g., such as a Smart Card, Smart Disk or a MCIA device... (Column 2, lines 1-5)." Smart Card, Smart Disk and MCIA devices are Integrated Circuits (IC's).

Claims 4 and 8 recite the limitations of a comparator (or "comparison circuitry") to verify the value (or number) written to storage is, in fact, the value given from the RNG. A write-verify process is the process of determining whether a value written to storage is the value that was intended to be written by comparing the respective values. Fischer's invention has verify-by-comparison logic that is stated as, "The entity which verifies the signature performs the following steps. The signature operation is verified to show that it correctly reflects the data which was signed and that is was correctly composed with the 'purported' date/time. A hash of the value **10** (output **508**), the date **504** and the seal **506** are input to verify the signature operation at **510**. (Column 12, lines 7-16)." Verifying a signature, per Fischer, is the processes of comparing the values: "If the seal **506** does *correctly reflect the data*, then processing continues... (Emphasis added, column 12, lines 16-17)." Checking whether data is "correctly reflected" is a comparison procedure.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. Claims 2, 3, 6, 7 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (U.S. Patent No. 5,422,953) and Brown et al. (U.S. Patent No. 4,853,884).

Claims 2, 3, 6, 7 and 10 recite "circuitry for detecting undesirable random numbers," wherein said circuitry determines the "1" to "0" ratio of a random value (number/key) and compares the determined ratio to a threshold value. Claim 10 further recites the limitation of generating a new random number in response to an undesired random number (i.e., generating a new random number if the ratio is outside the threshold).

Fischer teaches the system and method of an integrated circuit with a RNG, permanent and inaccessible memory (storage) for a value from the RNG, comparing a

Art Unit: 2139

written (stored) value to the respective generated value. (Previously shown per 35 U.S.C. 102(b) rejection, *supra*.) However, Fischer fails to teach the use of bit ratios (ones-to-zero's) to determine the acceptability of a generated random number, and regenerating a random number if the previous random number is determined as "undesirable" or outside the bit ratio threshold.

Brown et al. teach a "Random Number Generator with Digital Feedback. (Title)." Comparing the bit ratio (ones-to-zero's) of a generated random number to a threshold value is summarized by Brown et al. as, "A microprocessor feedback circuit monitors the random number output and produces the input control signal in response to the difference between the degree of randomness of the output signal and that of a pre-determined statistical distribution. [...] In the preferred embodiment, the microprocessor tests the ratio of ONES bits to ZERO bits of the random number such that a desired 1:1 ONES/ZERO ratio is approximated. (Abstract)." Approximation of said ratio is accomplished by reiteration of the random number generation after recalculation of parameters used to determine said random number. (Column 2, lines 20-25). Please also see column 2, lines 34-45.

It would have been obvious at the time the invention was made to one having ordinary skill in the art to combine the teachings of Fischer and Brown et al. by incorporating the random number acceptability test of Brown et al. into the secured-RNG device of Fischer because external (outside the IC) acceptability-verification of the random value (number/key) is not practical given the security protections of the memory where the random value is stored (within Fischer). Further, verification of the

Art Unit: 2139

randomness of the random value is beneficial because "[An] anomaly complicates a limiter design, since the known technique of eliminating the average DC component by AC coupling the zener diode noise output will not result in a balanced data stream of ONES and ZEROS. (Column 1, lines 57-61)."

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Bishop et al. (Patent No. 3,961,169) teaches "A biased sequence of binary bits is produced such that the probability that any randomly selected bit will be a "1" is equal to a preselected desired number. (Abstract)." Bishop et al. present a random-bit-stream-producing device, as opposed to a set-width RNG presented within the art cited, using the technique of one-to-zero ratio verifying.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kent L. Williams whose telephone number is 571-270-1376. The examiner can normally be reached on Mon-Fri 7:00-4:30 with Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2139

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kent Williams
3/2/2007

Taghi J. Arani
Primary Examiner
Taghi J. Arani
3/2/07